CLAIMS

I/We claim:

1.   A method for providing access to an application, comprising the
5   steps of:

encrypting at least one authentication sequence in a computer
system using a first network identifier as an encryption key;

storing the encrypted at least one authentication sequence in a
memory accessible to the computer system;

10   decrypting the encrypted at least one authentication sequence
using a second network identifier as a decryption key, the second network
identifier being procured after storing the encrypted at least one authentication
sequence; and

performing an expedited login task to access the application with
15   the at least one authentication sequence if the decryption of the at least one
authentication sequence is successful.

2.   The method of claim 1, further comprising the step of deleting the
20   encrypted at least one authentication sequence from the memory upon a failure
to successfully decrypt the encrypted at least one authentication sequence
using the second network identifier as a decryption key.

25   3.   The method of claim 1, wherein the step of performing the
expedited login task to access the application with the at least one
authentication sequence further comprises the steps of:

executing an automated login to access the application using the
at least one authentication sequence; and

30   executing the application if the automated login is successful.

4.   The method of claim 1, wherein the step of performing the expedited login task to access the application with the at least one authentication sequence further comprises the steps of:

presenting an application login interface to a user with the at least one authentication sequence inserted in the application login interface; and

executing the application in the computer system upon a generation of an input associated with the application login interface.

5.   The method of claim 1, further comprising the step of procuring the first network identifier, the first network identifier being a network address that varies based upon a network coupling status of the computer system.

6.   The method of claim 1, further comprising the step of procuring the first network identifier by examining an amount of data traffic on a network coupled to the computer system to obtain a network identification.

7.   The method of claim 1, further comprising the step of procuring the first network identifier by determining a physical proximity of the computer system to the location of a predefined network.

8.   A program embodied in a computer readable medium for providing access to an application, comprising:

code that procures a first network identifier associated with a network coupling status of a computer system;

5   code that encrypts at least one authentication sequence using the first network identifier as an encryption key;

code that stores the encrypted at least one authentication sequence in a memory;

code that procures a second network identifier after storing the

10   encrypted at least one authentication sequence;

code that decrypts the encrypted at least one authentication sequence using the second network identifier as a decryption key; and

code that executes an expedited login task to access the application with the at least one authentication sequence if the decryption of the

15   at least one authentication sequence is successful.

9.   The program embodied in the computer readable medium of claim 8, further comprising code that deletes the encrypted at least one authentication

20   sequence from the memory upon a failure to successfully decrypt the encrypted at least one authentication sequence using the second network identifier as a decryption key.

25   10.   The program embodied in the computer readable medium of claim 8, wherein the expedited login task to access the application with the at least one authentication sequence further comprises:

code that performs an automated login to access the application using the at least one authentication sequence; and

30   code that executes the application if the automated login is successful.

11. The program embodied in the computer readable medium of claim 8, wherein the expedited login task to access the application with the at least one authentication sequence further comprises:

code that presents an application login interface to a user with the at least one authentication sequence inserted in the application login interface; and

code that executes the application in the computer system upon a generation of an input associated with the application login interface.

10

12. The program embodied in the computer readable medium of claim 8, wherein the code that procures the first network identifier associated with the network coupling status of the computer system further comprises code that procures a network address as the network identifier, wherein the network address varies based upon a network coupling status of a computer system.

13. The program embodied in the computer readable medium of claim 8, wherein the code that procures the first network identifier associated with the network coupling status of the computer system further comprises code that procures the first network identifier by examining an amount of data traffic on a network coupled to the computer system to obtain a network identification.

14. The program embodied in the computer readable medium of claim 8, wherein the code that procures the first network identifier associated with the network coupling status of the computer system further comprises code that procures the first network identifier by determining a physical proximity of the computer system to the location of a predefined network.

30

15.   A system for providing access to an application, comprising:

a processor circuit having a processor and a memory;

the application stored in the memory and executable by the processor;

5   a secure login controller stored in the memory and executable by the processor, the secure login controller further comprising:

logic that procures a first network identifier associated with a network coupling status of the processor circuit;

logic that encrypts at least one authentication sequence

10   using the first network identifier as an encryption key;

logic that stores the encrypted at least one authentication sequence in the memory;

logic that procures a second network identifier after storing the encrypted at least one authentication sequence;

15   logic that decrypts the encrypted at least one authentication sequence using the second network identifier as a decryption key; and

logic that executes an expedited login task to access the application with the at least one authentication sequence if the decryption of the at least one authentication sequence is successful.

20

16.   The system of claim 15, further comprising logic that deletes the encrypted at least one authentication sequence from the memory upon a failure to successfully decrypt the encrypted at least one authentication sequence

25   using the second network identifier as a decryption key.

30

17.   The system of claim 15, wherein the expedited login task to access the application with the at least one authentication sequence further comprises:

logic that performs an automated login to access the application using the at least one authentication sequence; and

logic that executes the application if the automated login is successful.

18.   The system of claim 15, wherein the expedited login task to access the application with the at least one authentication sequence further comprises:

logic that presents an application login interface to a user with the at least one authentication sequence inserted in the application login interface; and

logic that executes the application in the computer system upon a generation of an input associated with the application login interface.

19.   The system of claim 15, wherein the logic that procures the first network identifier associated with the network coupling status of the processor circuit further comprises logic that procures a network address as the network identifier, wherein the network address varies based upon whether the processor circuit is coupled to one of a number of predefined networks.

20.   A system for providing access to an application, comprising:

means for procuring a first network identifier associated with a network coupling status of a computer system;

means for encrypting at least one authentication sequence using

5   the first network identifier as an encryption key;

means for storing the encrypted at least one authentication sequence in the memory;

means for procuring a second network identifier after storing the encrypted at least one authentication sequence;

10   means for decrypting the encrypted at least one authentication sequence using the second network identifier as a decryption key; and

means for executing an expedited login task to access the application with the at least one authentication sequence if the decryption of the at least one authentication sequence is successful.

15

21.   The system of claim 20, further comprising means for deleting the encrypted at least one authentication sequence from the memory upon a failure to successfully decrypt the encrypted at least one authentication sequence

20   using the second network identifier as a decryption key.

22.   The system of claim 20, wherein the expedited login task to access the application with the at least one authentication sequence further

25   comprises means for performing an automated login to access the application using the at least one authentication sequence.

30

23.   The system of claim 20, wherein the expedited login task to access the application with the at least one authentication sequence further comprises:

means for presenting an application login interface to a user with the at least one authentication sequence inserted in the application login interface; and

means for executing the application in the computer system upon a generation of an input associated with the application login interface.